

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

Payson Clarke and Stacey Sanchez, on)	
behalf of themselves and all others similarly)	
situated individuals,)	
)	
Plaintiffs,)	
)	Case No.
v.)	
)	
Verisource Services, Inc.,)	
)	
Defendant.		

INDEX

Defendant Verisource Services, Inc. is filing the following items with its
Notice of Removal:

- Section A: Notice of Removal
- Section B: Docket Report
- Section C: Class Action Petition with Exhibit 1
- Section D: Request for Issuance
- Section E: Citation (Executed) Verisource Services, Inc.
- Section F: Civil Case Information Sheet

Dated: October 1, 2024

Respectfully submitted,

/s/ Amanda N. Harvey

Amanda N. Harvey
State Bar No. 24046038

aharvey@mullen.law

Kayleigh J. Watson
State Bar No. 24102632

kwatson@mullen.law

MULLEN COUGHLIN LLC

1452 Hughes Rd Suite 200

Grapevine, TX 76051

Telephone: 267/930-1697

Facsimile: 267/930-4771

*Counsel to Defendant Verisource Services,
Inc.*

Court of Texas (the “Petition”). A copy of the Petition is attached as Exhibit A to this Notice.

2. The Summons and Complaint were served on Verisource on September 13, 2024.

3. According to the Complaint, Plaintiffs are citizens of Texas. Pet. ¶¶ 11-12.

4. Verisource is a Texas corporation headquartered in Houston, Texas. *Id.* at ¶ 13.

5. In the Petition, Plaintiffs allege that Plaintiffs and Class Members had their sensitive information exposed after an unknown actor accessed Defendants’ systems. *Id.* at ¶ 94.

6. Plaintiffs assert causes of action for negligence, negligence *per se*, breach of third-party beneficiary contract, unjust enrichment, and declaratory and injunctive judgment. *Id.* at ¶¶ 123-192.

7. Plaintiffs seek to represent a putative class consisting of “[a]ll persons who were sent a Notice of Data Breach Letter from VSI or one of VSI’s customers after the Data Breach.” *Id.* at ¶ 113.

8. Plaintiffs seek recovery, for themselves and members of the putative class, of “monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs . . .”. *Id.* at Prayer ¶ b.

9. Verisource has not filed a responsive pleading or otherwise responded to the Complaint in the state court action.

10. This notice of removal is timely because it has been filed within thirty (30) days of September 13, 2024, which is the date on which Verisource accepted service of the Petition.

11. Removal to the federal court is proper because it is the “district ...embracing the place” in which the state court action is pending. 28 U.S.C. § 1441(a).

12. Verisource has conferred with Plaintiffs’ counsel regarding the filing of this removal and Plaintiffs do not oppose the removal of the case.

II. GROUNDS FOR REMOVAL

13. Jurisdiction in federal court is appropriate under 28 U.S.C. § 1332(d), as amended by the Class Action Fairness Act of 2005 (“CAFA”) because this matter involves a putative class action, and: (1) the number of proposed class members is 100 or more; (2) at least one member of the class resides outside of Texas, and (3) the amount in controversy as pled exceeds \$5 million in the aggregate, exclusive of interest and costs. *See* 28 U.S.C. §§ 1332(d).

A. At Least One Class Member of the Class Resides Outside Texas

14. At least one class member of the class resides outside the state of Texas. There have been 112,726¹ people notified and, out of the people notified, 55,312 reside in Texas. *Id.* at ¶ 1.

B. The Proposed Class Consists of More than 100 Members

15. Plaintiffs bring this action on behalf of a putative class. To date Verisource has notified approximately 112,726 individuals who were potentially impacted.

C. The Amount in Controversy Exceeds \$5,000,000

16. The amount in controversy exceeds \$5 million in the aggregate, exclusive of interest and costs. Verisource has notified 112,726 individuals.

17. Plaintiffs seek economic damages relating to a number of items, as set forth above in paragraph 8. Among other things, Plaintiffs incurred “out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time.” Pet. ¶ 146.

18. Depending on the subscription level, an annual subscription to the widely utilized identity theft protection product Norton LifeLock costs between

¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

\$89.99 and \$239.88 for the first year, with renewal at an annual cost of \$124.99 to \$339.99.²

19. A single year of the Norton LifeLock product for the proposed class of 112,726 individuals would cost between \$10,144,212.70 and \$27,040,712.90. This calculation does not even take into account Plaintiffs' other alleged damages.

20. Therefore, without conceding that either Plaintiffs or any member of the proposed class is entitled to any damage award, or the class certification is proper and warranted, and relying on Plaintiffs' allegations without admission, Defendant states that the matter in controversy exceeds the sum or value of \$5,000,000 if the class were to be certified, for those amounts sought in the Complaint.

21. Verisource therefore removes this matter to this Court pursuant to 28 U.S.C. §§ 1332(d)(2), 1332(d)(5)(B), and 1332(d)(6).

22. This Notice of Removal is signed pursuant to Rule 11 of the Federal Rules of Civil Procedure. 28 U.S.C. § 1446(d).

23. A copy of this Notice of Removal is being served upon counsel for Plaintiffs, and upon filing this Notice of Removal in this Court, Verisource will file a true and correct copy of the Notice with the Clerk of Court in County of Harris, District Court of Texas and will give written notice to Plaintiffs. *See* 28 U.S.C. § 1446(d).

² <https://lifelock.norton.com/products> (last accessed on September 20, 2024).

Respectfully submitted,

/s/ Amanda N. Harvey

Amanda N. Harvey

State Bar No. 24046038

aharvey@mullen.law

Kayleigh J. Watson

State Bar No. 24102632

kwatson@mullen.law

MULLEN COUGHLIN LLC

1452 Hughes Rd Suite 200

Grapevine, TX 76051

Telephone: 267/930-1697

Facsimile: 267/930-4771

*Counsel to Defendant Verisource Services,
Inc.*

Dated: October 1, 2024

2024-58710

COURT: 234th

FILED DATE: 8/30/2024

CASE TYPE: Other Injury or Damage



**CLARKE, PAYSON (ON BEHALF OF THEMSELVES AND ON
BEHAL OF ALL OTHER**

Attorney: FEDERMAN, WILLIAM B.

VS.

VERISOURCE SERVICES INC

Docket Sheet Entries

Date

Comment

HCDistrictclerk.comCLARKE, PAYSON (ON BEHALF OF THEMSELVES
AND ON BEHAL OF ALL OTHER vs. VERISOURCE
SERVICES INC

9/30/2024

Cause: 202458710 CDI: 7 Court: 234

DOCUMENTS

Number	Document	Post Jdgm	Date	Pgs
116559202	Citation (Executed) VERISOURCE SERVICES INC		09/19/2024	2
116235799	Civil Case Information Sheet		08/30/2024	1
116235800	Request For Issuance		08/30/2024	1
116251244	Class Action Petition		08/30/2024	49
-> 116251245	Exhibit 01		08/30/2024	3

2024-58710 / Court: 234

CAUSE NO. _____

PAYSON CLARKE AND STACEY SANCHEZ, on behalf of themselves and on behalf of all other similarly situated individuals,

Plaintiffs,

v.

VERISOURCE SERVICES, INC.,

Defendant.

DISTRICT COURT OF TEXAS

JUDICIAL DISTRICT
HARRIS COUNTY

CLASS ACTION PETITION

Plaintiffs Payson Clarke and Stacey Sanchez (“Plaintiffs”), individually and on behalf of all other similarly situated individuals (the “Class” or “Class Members,” as defined below), by and through their undersigned counsel, file this Class Action Petition against Verisource Services, Inc. (“VSI” or “Defendant”) and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of their counsel as to all other matters.

I. DISCOVERY CONTROL PLAN

Discovery is intended to be conducted under level three pursuant to Texas Rule of Civil Procedure 190.4.

II. NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit against VSI for its negligent failure to protect and safeguard Plaintiffs' and the Class's highly sensitive personally identifiable information ("PII"). As a result of VSI's negligence and insufficient data security, cybercriminals easily infiltrated Defendant's inadequately protected computer systems and stole the PII of Plaintiffs and the Class (approximately 55,312 Texas residents) (the "Data Breach" or "Breach").¹ Now, Plaintiffs' and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. According to VSI, "[o]n February 28, 2024, VSI became aware of unusual activity on our network environment."²

3. After discovering the Data Breach, VSI hired independent cybersecurity personnel to undertake an investigation.³

4. "The investigation subsequently revealed that **certain personal information was acquired without authorization** on or about February 27, 2024."⁴

5. VSI then commenced a review of the affected data to determine whether any sensitive data was involved and whether personal information may have been affected. The

¹ <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage>.

² <http://www.verisource.com/Incident.html>

³ *Id.*

⁴ *Id.* (emphasis added).

review confirmed that names, dates of birth, and Social Security numbers were stolen during the Data Breach (collectively, “Private Information”).⁵

6. Defendant began sending Notice of Data Breach Letters to victims of the Data Breach in or around August 20, 2024.⁶

7. Due to Defendant’s negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

8. Now, and for the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

9. In sum, Plaintiffs and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because (i) VSI failed to protect Plaintiffs’ and the Class’s PI, allowing a massive and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach, stole Private Information that they will sell on

⁵ *Id.*

⁶ *See* Exs. 1 and 2.

the dark web; (iii) VSI failed to provide any assurance that it paid a ransom to prevent Plaintiffs' and the Class's data from being released on the dark web; and (iv) VSI offered credit monitoring to Plaintiffs and the Class, an offer it need not make if no PII was stolen and at risk of misuse.

10. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

III. THE PARTIES

11. Plaintiff **Payson Clarke** is an individual domiciled in Richmond, Texas. Plaintiff Clarke received a Notice of Data Breach Letter from VSI dated August 20, 2024, notifying him that his Social Security number and name were "acquired without authorization."⁷

12. Plaintiff **Stacey Sanchez** is an individual domiciled in Richmond, Texas. Plaintiff Sanchez received a Notice of Data Breach Letter from VSI dated August 20, 2024, notifying her that her Social Security number and name were "acquired without authorization

13. Defendant **Verisource Services, Inc.** is a Texas domestic for-profit corporation with a principal office address located at 7600 West Tidwell, Suite 700, Houston, TX 77040. Defendant's registered agent is Kathleen J. Lee, who is located at

⁷ See Ex. 1.

7600 West Tidwell, Suite 700, Houston, TX 77040.

IV. JURISDICTION AND VENUE

14. Jurisdiction before this Court is proper because the amount in controversy satisfies the jurisdictional limits of this Court, and all parties are subject to personal jurisdiction in Texas.

15. This Court has personal jurisdiction over Defendant because Defendant is a Texas domestic limited liability company; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

16. Venue is proper in Harris County under Tex. Civ. Prac. And Rem. Code § 15.002(a) because the causes of action pleaded herein arose in substantial part in Harris County and Defendant's principal place of business is located in Harris County.

V. FACTUAL ALLEGATIONS

A. Defendant and its Collection of Plaintiffs' and the Class's PII.

17. Founded in 1997, VSI is a business services company based out of Houston, Texas. VSI provides employee benefits administrative and enrollment services to employers.⁸

⁸ <http://verisource.com/Home/About/2>.

18. VSI also provides HR outsourcing services, direct billing administration services, and dependent verification services.⁹

19. VSI employs more than 25 people and generates approximately \$7 million in annual revenue.¹⁰

20. Plaintiffs and the Class are employees of a company that uses VSI's services or a beneficiary or dependent of an employee who works at a company that uses VSI's services.¹¹

21. VSI could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

22. In the ordinary course of business, VSI receives the PII of individuals, such as Plaintiffs and the Class, from the entities and individuals that utilize VSI's services.

23. VSI obtains, collects, uses, and derives a benefit from the PII of Plaintiffs' and Class Members. VSI uses the PII it collects to provide services, making a profit therefrom. VSI would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's PII.

24. By collecting Plaintiffs' and the Class's PII, VSI assumed legal and equitable duties to Plaintiffs and the Class to protect and safeguard their PII from unauthorized access and intrusion.

25. VSI recognized this duty but failed to take it seriously.

⁹ <http://verisource.com/Services/Index/3>.

¹⁰ <https://www.zoominfo.com/c/verisource-services-inc/40763428>.

¹¹ Exs. 1–2.

26. As a result, Plaintiffs' and Class Members' PII was accessed and stolen from VSI's inadequately secured data systems in a massive and preventable Data Breach.

B. VSI's Massive and Preventable Data Breach.

27. On February 28, 2024, VSI became aware of unusual activity in its network environment.¹²

28. Upon discovering this activity, VSI claims it took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts.¹³

29. "The investigation subsequently revealed that certain personal information was **acquired without authorization** on or about February 27, 2024."¹⁴

30. VSI reviewed the affected data to determine whether any sensitive data was involved and whether personal information may have been affected.¹⁵

31. On August 12, 2024, that review concluded, and confirmed that certain personal information was involved.¹⁶

32. The Private Information stolen in the Data Breach included at least: names, dates of birth, and Social Security Numbers.¹⁷

33. Despite discovering the Data Breach on February 28, 2024, VSI did not begin notifying individuals of the Data Breach until on or around August 20, 2024.¹⁸

¹² <http://www.verisource.com/Incident.html>.

¹³ *Id.*

¹⁴ *Id.* (emphasis added).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *See* Exs. 1–2.

34. In recognition of the severity of the Data Breach, and the imminent risk of harm Plaintiffs and the Class face, VSI made a measly offering of twelve (12) months of identity theft protection services.¹⁹ Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has *already occurred*.

35. All in all, VSI failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access and exploitation.

36. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

C. Cybercriminals Have Used and Will Continue to Use Plaintiffs' and the Class's PII to Defraud Them.

37. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

38. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.²⁰

39. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of

¹⁹ *Id.*

²⁰ *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.²¹ These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

40. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.*²²

[Emphasis added.]

41. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.²³

42. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of running targeted cyberattacks against companies

²¹ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

²² *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

²³ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at <https://www.gao.gov/products/gao-07-737>.

like VSI is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

43. Indeed, a social security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.²⁴

44. “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”²⁵

45. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to PII, **they will use it**.²⁶

46. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁷

²⁴ Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

²⁵ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

²⁶ Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), <https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info>.

²⁷ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at <https://www.gao.gov/products/gao-07-737>.

47. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.²⁸

48. With this Data Breach, identity thieves have already started to prey on the VSI Data Breach victims, and we can anticipate that this will continue.

49. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.²⁹

50. Defendant's offer of one year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures.

51. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

52. Once the twelve months have expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to VSI's gross negligence.

²⁸ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

²⁹ *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), available at <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

53. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (i.e., fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.³⁰ Nor can an identity monitoring service remove personal information from the dark web.³¹

54. “The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it.”³²

55. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

56. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police

³⁰ See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

³¹ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.

³² *Id.*

reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

57. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

- a. Actual identity theft;
- b. Trespass, damage to, and theft of their personal property including PII;
- c. Improper disclosure of their PII;
- d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII;
- f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
- h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

- i. The loss of use of and access to their credit, accounts, and/or funds;
- j. Damage to their credit due to fraudulent use of their PII; and/or
- k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

58. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' and the Class's Private Information.

59. Plaintiffs and Class Members also have an interest in ensuring that their Private Information that was provided to VSI is removed from all VSI servers, systems, and files.

60. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members woefully inadequate identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

61. Defendant further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur because

it advised individuals to enroll in credit monitoring, place a fraud alert/security freeze on credit files, and obtain a free credit report.³³

62. Defendant further acknowledged its did not have adequate data security at the time of the Breach because Defendant claims to have “implemented several measures to enhance [its] security posture and reduce the risk of similar future incidents.”³⁴

63. These enhanced protections should have been in place before the Data Breach.

64. At VSI’s suggestion, Plaintiffs and the Class are desperately trying to mitigate the damage that VSI has caused them.

65. Given the kind of Private Information VSI made accessible to hackers, however, Plaintiffs and the Class are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.³⁵

66. None of this should have happened because the Data Breach was entirely preventable.

³³ Exs. 1–2.

³⁴ *Id.*

³⁵ *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

D. Defendant was Aware of the Risk of Cyberattacks.

67. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,³⁶ Yahoo,³⁷ Marriott International,³⁸ Chipotle, Chili's, Arby's,³⁹ and others.⁴⁰

68. "Payroll companies are no stranger to being cybersecurity targets and victims."⁴¹

69. "The payroll industry is a lucrative target for cybercriminals. Just in the United States alone, the industry is worth \$58.3 billion. That makes them more vulnerable to cybersecurity threats because they store sensitive data about their employees, such as social security numbers, bank account information, and salary information. Payroll companies need to understand the cyber threats they are at risk of encountering."⁴²

³⁶ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.

³⁷ Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoononline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

³⁸ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> (last visited Oct. 9, 2023).

³⁹ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b>.

⁴⁰ See, e.g., Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), <https://www.csoononline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

⁴¹ <https://www.cybrella.io/post/how-payroll-companies-can-reduce-risk-of-a-cyberattack>.

⁴² *Id.*

70. “Small payroll companies struggle with cyber hygiene often due to staffing limitations. In many cases, they don't have the capacity or specialization to implement a comprehensive cybersecurity program, leaving their systems vulnerable to cyberattacks. The first step in any cybersecurity journey should be to develop a cybersecurity framework to follow, such as that developed by the National Institute Standards of Technology (NIST).”⁴³

71. VSI should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained.

72. VSI was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

E. VSI Could Have Prevented the Data Breach.

73. Data breaches are preventable.⁴⁴ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”⁴⁵ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised”⁴⁶

⁴³ *Id.*

⁴⁴ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

⁴⁵ *Id.* at 17.

⁴⁶ *Id.* at 28.

74. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”⁴⁷

75. In a data breach like this, many failures laid the groundwork for the Breach.

76. The FTC has published guidelines that establish reasonable data security practices for businesses.

77. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.⁴⁸

78. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

79. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for

⁴⁷*Id.*

⁴⁸ *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

80. According to information and belief, VSI failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

81. Upon information and belief, VSI also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

82. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."⁴⁹

83. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

⁴⁹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁵⁰

84. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

⁵⁰ *Id.* at 3–4.

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous

(legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁵¹

85. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audit; remove privileged credentials

⁵¹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://www.cisa.gov/news-events/news/protecting-against-ransomware>.

- **Thoroughly investigate and remediate alerts**
 - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
 - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
 - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**
 - Use Windows Defender Firewall
 - Enable tamper protection
 - Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁵²

86. Given that Defendant was storing the PII of more than 6 million individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

87. Specifically, among other failures, VSI had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.⁵³

88. Moreover, it is a well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed.

89. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁵⁴ VSI, rather than following this basic standard of care, kept thousands of individuals’ unencrypted PII indefinitely.

⁵² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

⁵³ See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

⁵⁴ *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

90. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

91. Further, the scope of the Data Breach could have been dramatically reduced had VSI utilized proper record retention and destruction practices.

F. Plaintiffs' Individual Experience

Plaintiff Payson Clarke

92. Plaintiff Clarke received a Notice of Data Breach Letter from Defendant informing him that his highly confidential Private Information was compromised in the Data Breach.⁵⁵

93. Defendant was in possession of Plaintiff Clarke's Private Information before, during, and after the Data Breach.

94. Because of the Data Breach, there is no doubt Plaintiff Clarke's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had accessed Defendant's systems, but it confirmed that the unauthorized criminal actor acquired files containing highly sensitive PII.⁵⁶ As such, Plaintiff Clarke and the Class are at an imminent risk of identity theft and fraud.

95. As a result of the Data Breach, Plaintiff Clarke has already expended over **100 hours** of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach,

⁵⁵ Ex. 1.

⁵⁶ *Id.*

including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information. Additionally, Plaintiff Clarke also placed a security freeze with the credit bureaus.

96. Plaintiff Clarke has also experienced an increase in phishing text messages and emails he attributes to the Data Breach.

97. Plaintiff Clarke places significant value on the security of his Private Information and does not readily disclose it. Plaintiff Clarke has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

98. Plaintiff Clarke has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Clarke, and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Clarke and the Class.

99. Knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals has caused Plaintiff Clarke great anxiety beyond mere worry. Specifically, Plaintiff Clarke has lost hours of sleep, is in a constant state of stress, is very

frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

100. Plaintiff Clarke has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

101. Plaintiff Clarke has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Clarke should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Stacey Sanchez

102. Plaintiff Sanchez received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.⁵⁷

103. Defendant was in possession of Plaintiff Sanchez's Private Information before, during, and after the Data Breach.

104. Because of the Data Breach, there is no doubt Plaintiff Sanchez's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had accessed Defendant's systems, but it confirmed that the unauthorized criminal actor acquired files containing highly sensitive PII. As such, Plaintiff Sanchez and the Class are at an imminent risk of identity theft and fraud.

105. As a result of the Data Breach, Plaintiff Sanchez has already expended over **100 hours** of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information. Additionally, Plaintiff Sanchez also placed a security freeze with the credit bureaus.

⁵⁷ Ex. 2.

106. Plaintiff Sanchez has also experienced an increase in phishing text messages and emails she attributes to the Data Breach.

107. Plaintiff Sanchez places significant value on the security of her Private Information and does not readily disclose it. Plaintiff Sanchez has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

108. Plaintiff Sanchez has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Sanchez, and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Sanchez and the Class.

109. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Sanchez great anxiety beyond mere worry. Specifically, Plaintiff Sanchez has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

110. Plaintiff Sanchez has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention,

Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

111. Plaintiff Sanchez has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Sanchez should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

VI. CLASS ACTION ALLEGATIONS

112. Plaintiffs incorporates by reference all preceding paragraphs as if fully restated here.

113. Plaintiffs brings this action against VSI on behalf of himself and all other individuals similarly situated under Texas Rule of Civil Procedure 42. Plaintiffs asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

All persons who were sent a Notice of Data Breach Letter from VSI or one of VSI's customers after the Data Breach.

114. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

115. Plaintiffs reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

116. Plaintiffs anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

117. The proposed Class meets the requirements of Texas Rule of Civil Procedure 42.

118. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable.

119. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through VSI's uniform misconduct. VSI's inadequate data security gave rise to Plaintiffs' claims and are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of VSI.

120. **Adequacy:** Plaintiffs is an adequate representative of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

121. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress VSI's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

122. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;

- b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;
- c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;
- d. Whether VSI breached its duties to Plaintiffs and the Class;
- e. Whether VSI failed to provide adequate cyber security;
- f. Whether VSI knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;
- g. Whether VSI's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;
- h. Whether VSI was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;
- i. Whether VSI was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees and business associates;
- j. Whether VSI breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;
- k. Whether VSI failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;
- l. Whether VSI continues to breach duties to Plaintiffs and the Class;

- m. Whether Plaintiffs and the Class suffered injury as a proximate result of VSI's negligent actions or failures to act;
- n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and
- o. Whether VSI's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VII. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

- 123. Plaintiffs incorporates paragraphs 1–122 as though fully set forth herein.
- 124. VSI solicited, gathered, and stored the PII of Plaintiffs and Class Members.
- 125. Upon accepting and storing the PII of Plaintiffs and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.
- 126. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

127. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their PII, including names, Social Security numbers, and other PII.

128. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used for the provided purpose and that Defendant would destroy any PII that it was not required to maintain.

129. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

130. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

131. Plaintiffs and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

132. Defendant was aware of the fact that cybercriminals routinely target payroll companies like Defendant through cyberattacks in an attempt to steal customer and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

133. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the

Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

134. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

135. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs, and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PII was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiffs' and Class members' PII in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and
- d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

136. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

137. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

138. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' PII. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;
- b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
- c. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;
- d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- e. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their PII.

139. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

140. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices

and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

141. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members while it was within Defendant's possession and control.

142. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

143. Plaintiffs and Class members could have taken actions earlier had they been timely notified of the Data Breach.

144. Plaintiffs and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

145. Plaintiffs and Class members have suffered harm from the delay in notifying them of the Data Breach.

146. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII;

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

147. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

148. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

149. Plaintiffs incorporates paragraphs 1–122 as though fully set forth herein.

150. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and the Class.

151. The FTC Act prohibits “unfair practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant’s duty in this regard.

152. Defendant gathered and stored the PII of Plaintiffs and the Class as part of their business which affects commerce.

153. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

154. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs’ and Class members’ PII, and by failing to provide prompt notice without reasonable delay.

155. Defendant’s multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

156. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

157. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

158. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

159. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

160. Defendant's violations of the FTC Act constitute negligence *per se*.

161. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

162. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

163. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

**THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class)**

164. Plaintiffs incorporates paragraphs 1–122 as though fully set forth herein.

165. On information and belief, Defendant entered into written contracts to

provide financial services to companies.

166. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class and to timely and adequately notify them of the Data Breach.

167. According to information and belief, these contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, Plaintiffs and Class Members would be harmed.

168. Defendant breached the contracts entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

169. Plaintiffs and the Class were harmed by Defendant's breaches of contract, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

170. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

**FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)**

171. Plaintiffs incorporates paragraphs 1–122 as though fully set forth herein.

172. Plaintiffs allege this claim in the alternative to their breach of third-party beneficiary contract claim.

173. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs’ retained data and commercialized and used Plaintiffs’ and Class Members’ PII for business purposes.

174. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

175. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

176. Defendant failed to secure Plaintiffs’ and Class Members’ Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

177. Defendant acquired the PII through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiffs and Class Members had known that Defendant would not fund adequate data security practices, procedures,

and protocols to sufficiently monitor, supervise, and secure their PII, they would not have entrusted their Private Information to Defendant or obtained services from Defendant's clients.

178. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

179. Plaintiffs and Class Members have no adequate remedy at law.

180. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

181. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiffs' efforts to prevent from succeeding.

182. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

**FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)**

183. Plaintiffs incorporates paragraphs 1–122 as though fully set forth herein.

184. As previously alleged, Plaintiffs and members of the Class are entered into implied contracts with Defendant, which contracts require Defendant to provide adequate security for the PII collected from Plaintiffs and the Class.

185. Defendant owed and still owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' PII.

186. Upon reason and belief, Defendant still possesses the PII of Plaintiffs and the Class members.

187. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

188. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

189. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

190. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of

additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

191. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

192. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's

systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

- e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;
- f. Ordering that Defendant conduct regular database scanning and security checks; and
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Texas Rule of Civil Procedure 42, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;
- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
- e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- f. An award of such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiffs hereby demands a trial by jury on all appropriate issues raised in this Class Action Petition.

Dated: August 30, 2024

Respectfully submitted,

/s/ William B. Federman

William B. Federman

Tex. Bar No. 00794935

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

-and-

212 W. Spring Valley Rd.

Richardson, TX 75081

Telephone: (405) 235-1560

Fax: (214) 740-0112

wbf@federmanlaw.com

***Counsel for Plaintiff and the
Putative Class***

EXHIBIT 1



P.O. Box 989728
West Sacramento, CA 95798-9728



Payson Clarke

[Redacted]

Enrollment Code [Redacted]
To Enroll, Scan the QR Code Below:



Or Visit:

<https://register.idx.us/varsources>

August 20, 2024

Subject: Notice of Data Security Incident

Dear Payson Clarke:

We are writing to inform you about a recent data security incident experienced by VariSource Services, Inc. ("VSI") that may have involved your personal information. VSI provides employee administrative and benefit data management services for companies. You may be receiving this letter as an employee of a company that uses VSI's services or because that employer designated you as their beneficiary or dependent. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On February 28, 2024, VSI became aware of unusual activity that disrupted access to certain systems. Upon discovery, VSI immediately took steps to secure its network and engaged a leading, independent digital forensics and incident response firm to investigate what happened and whether any sensitive data may have been impacted. The investigation subsequently revealed certain personal information was acquired without authorization by an unknown actor on or about February 27, 2024. VSI undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on August 12, 2024. We then took steps to notify you of the incident as quickly as possible. Please note that VSI has no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information that was potentially impacted during this incident may have included your name, as well as your Social Security number.

What Are We Doing? As soon as VSI discovered the incident, we took the steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

We are also offering you access to complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: 12 months of credit and Cybercam monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



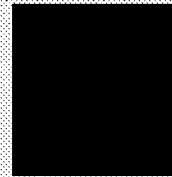
P.O. Box 989728
 West Sacramento, CA 95798-9728



Stacey Sanchez

[Redacted]

Enrollment Code [Redacted]
 To Enroll, Scan the QR Code Below:



Or Visit:
<https://verisource.idx.us/verisource>

August 28, 2024

Subject: Notice of Data Security Incident

Dear Stacey Sanchez:

We are writing to inform you about a recent data security incident experienced by Verisource Services, Inc. ("VSI") that may have involved your personal information. VSI provides employee administrative and benefit data management services for companies. You may be receiving this letter as an employee of a company that uses VSI's services or because that employee designated you as their beneficiary or dependent. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On February 28, 2024, VSI became aware of unusual activity that disrupted access to certain systems. Upon discovery, VSI immediately took steps to secure its network and engaged a leading, independent digital forensics and incident response firm to investigate what happened and whether any sensitive data may have been impacted. The investigation subsequently revealed certain personal information was acquired without authorization by an unknown actor on or about February 27, 2024. VSI undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on August 12, 2024. We then took steps to notify you of the incident as quickly as possible. Please note that VSI has no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information that was potentially impacted during this incident may have included your name, as well as your Social Security number.

What Are We Doing? As soon as VSI discovered the incident, we took the steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

We are also offering you access to complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



I, Marilyn Burgess, District Clerk of Harris County, Texas certify that this is a true and correct copy of the original record filed and or recorded in my office, electronically or hard copy, as it appears on this date.

Witness my official hand and seal of office this September 30, 2024

Certified Document Number: 116251245 Total Pages: 3

Marilyn Burgess, DISTRICT CLERK
HARRIS COUNTY, TEXAS

In accordance with Texas Government Code 51.301 and 406.013 electronically transmitted authenticated documents are valid. If there is a question regarding the validity of this document and or seal please e-mail support@hcdistrictclerk.com

REQUEST FOR ISSUANCE

CAUSE NUMBER: _____

TYPE OF ISSUANCE: *E-FILING-YOU MUST ASSESS THE TYPE OF ISSUANCE, TYPE OF SERVICE, SERVICE FEES, AND COPY FEES ACCORDINGLY*

- ☒ CITATION
☐ PRECEPT
☐ TRO
☐ PROTECTIVE ORDER
☐ ABSTRACT OF JUDGMENT
☐ WRIT OF EXECUTION
☐ OTHER: _____

TYPE OF SERVICE:

- ☐ POTTER COUNTY SHERIFF *SERVICE FEE AND COPY FEE REQUIRED*
☐ CIVIL PROCESS SERVER-AUTHORIZED PERSON TO PICK-UP: _____
☐ POSTING *SERVICE FEE AND COPY FEE REQUIRED*
☐ PUBLICATION *SERVICE FEE REQUIRED*
☐ CERTIFIED MAIL *SERVICE FEE AND COPY FEE REQUIRED*
☐ TO BE MAILED TO PARTY REQUESTING SERVICE *SELF ADDRESSED STAMPED ENVELOPE AND/OR POSTAGE FEE REQUIRED*
☒ TO BE EMAILED TO PARTY REQUESTING SERVICES-**MUST INCLUDE EMAIL ADDRESS**

TITLE OF DOCUMENT: _____

FOR EACH PARTY SERVED YOU MUST ASSESS THE APPROPRIATE NUMBER OF COPIES OF THE DOCUMENT TO BE SERVED * UNLESS CLERK IS TO EMAIL, THEN NO COPY FEE IS REQUIRED*

FILE MARKED DATE OF DOCUMENT TO BE SERVED: ____/____/____

PARTY TO BE SERVED: (PLEASE FILL OUT A NEW REQUEST FORM PER PARTY TO BE SERVED)

NAME: Verisource Services, Inc., c/o Kathleen J. Lee, Registered Agent

ADDRESS: 7600 West Tidwell, Suite 700, Houston, TX 77040

AGENT, IF APPLICABLE: _____

PARTY/ATTORNEY REQUESTING SERVICE:

NAME: William B. Federman

MAILING ADDRESS: 212 W. Spring Valley Rd., Richardson, TX 75081

PHONE NUMBER: 405-235-1560 FAX NUMBER: 405-239-2112

EMAIL ADDRESS: wbf@federmanlaw.com; trp@federmanlaw.com



I, Marilyn Burgess, District Clerk of Harris County, Texas certify that this is a true and correct copy of the original record filed and or recorded in my office, electronically or hard copy, as it appears on this date.

Witness my official hand and seal of office this September 30, 2024

Certified Document Number: 116235800 Total Pages: 1

Marilyn Burgess, DISTRICT CLERK
HARRIS COUNTY, TEXAS

In accordance with Texas Government Code 51.301 and 406.013 electronically transmitted authenticated documents are valid. If there is a question regarding the validity of this document and or seal please e-mail support@hcdistrictclerk.com

AFFIDAVIT OF SERVICE

State of Texas

County of Harris

234th Judicial District Court

Case Number: 2024-58710

Plaintiff:

Payson Clarke and Stacey Sanchez, on behalf of themselves and on behalf of all other similarly situated individuals

vs.

Defendant:

Verisource Services, Inc.

For:

Federman & Sherwood
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120

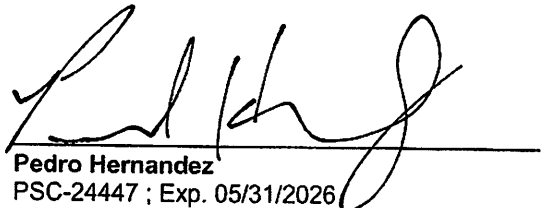
Received by Pedro Hernandez on the 6th day of September, 2024 at 10:03 am to be served on **Verisource Services Inc. by serving its Registered Agent, Kathleen J. Lee, 7600 W Tidwell Rd, Ste 700, Houston, Harris County, TX 77040.**

I, Pedro Hernandez, being duly sworn, depose and say that on the **13th day of September, 2024 at 12:39 pm, I:**

delivered to a **BUSINESS ENTITY, BY AND THROUGH ITS REGISTERED AGENT**, by delivering a true copy of the **Citation and Class Action Petition with Exhibit 1** with the date of service endorsed thereon by me, to: **Kathleen J. Lee as Registered Agent for Verisource Services Inc.** at the address of: **7600 W Tidwell Rd, Ste 700, Houston, Harris County, TX 77040.**

Description of Person Served: Age: 60s, Sex: F, Race/Skin Color: White, Height: -, Weight: -, Hair: Gray, Glasses: N

I certify that I am over the age of 18, I am not a party to the suit, and I am a disinterested person with no interest in the outcome of the suit. The facts stated in this affidavit are within my personal knowledge and are true and correct. I delivered the listed documents with the date of service endorsed thereon by me and informed the recipient of the contents therein, in compliance with state statutes.

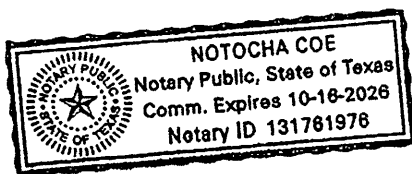


Pedro Hernandez
PSC-24447 ; Exp. 05/31/2026

Subscribed and Sworn to before me on the 17th day of September, 2024 by the affiant who is personally known to me.



NOTARY PUBLIC



Austin Process LLC
1100 Nueces
Austin, TX 78701
(512) 480-8071

Our Job Serial Number: MST-2024007945
Ref: Clarke, et al. v. Verisource

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

William Federman
 Bar No. 794935
 wbf@federmanlaw.com
 Envelope ID: 92241253
 Filing Code Description: No Fee Documents
 Filing Description: Affidavit of Service
 Status as of 9/20/2024 7:48 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Tiffany Peintner		trp@federmanlaw.com	9/19/2024 4:25:53 PM	SENT
William B.Federman		wbf@federmanlaw.com	9/19/2024 4:25:53 PM	SENT
Kennedy M.Brian		kpb@federmanlaw.com	9/19/2024 4:25:53 PM	SENT
Administrative Administrative		law@federmanlaw.com	9/19/2024 4:25:53 PM	ERROR



I, Marilyn Burgess, District Clerk of Harris County, Texas certify that this is a true and correct copy of the original record filed and or recorded in my office, electronically or hard copy, as it appears on this date.

Witness my official hand and seal of office this September 30, 2024

Certified Document Number: 116559202 Total Pages: 2

Marilyn Burgess, DISTRICT CLERK
HARRIS COUNTY, TEXAS

In accordance with Texas Government Code 51.301 and 406.013 electronically transmitted authenticated documents are valid. If there is a question regarding the validity of this document and or seal please e-mail support@hcdistrictclerk.com

CIVIL CASE INFORMATION SHEET

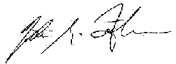
CAUSE NUMBER (FOR CLERK USE ONLY): _____

COURT (FOR CLERK USE ONLY): _____

STYLED Payson Clarke and Stacey Sanchez v. Verisource Services, Inc.

(e.g., John Smith v. All American Insurance Co; In re Mary Ann Jones; In the Matter of the Estate of George Jackson)

A civil case information sheet must be completed and submitted when an original petition or application is filed to initiate a new civil, family law, probate, or mental health case or when a post-judgment petition for modification or motion for enforcement is filed in a family law case. The information should be the best available at the time of filing. This sheet, approved by the Texas Judicial Council, is intended to collect information that will be used for statistical purposes only. It neither replaces nor supplements the filings or service of pleading or other documents as required by law or rule. The sheet does not constitute a discovery request, response, or supplementation, and it is not admissible at trial.

1. Contact information for person completing case information sheet:		Names of parties in case:		Person or entity completing sheet is:	
Name: William B. Federman	Email: wbf@federmanlaw.com	Plaintiff(s)/Petitioner(s): Payson Clarke		<input type="checkbox"/> Attorney for Plaintiff/Petitioner <input type="checkbox"/> Pro Se Plaintiff/Petitioner <input type="checkbox"/> Title IV-D Agency <input type="checkbox"/> Other: _____	
Address: 212 W. Spring Valley Rd.	Telephone: 405-235-1560	Defendant(s)/Respondent(s): Verisource Services, Inc.		Additional Parties in Child Support Case: Custodial Parent: _____ Non-Custodial Parent: _____ Presumed Father: _____	
City/State/Zip: Richardson, TX 75081	Fax: 405-235-1560				
Signature: 	State Bar No: 00794935				
[Attach additional page as necessary to list all parties]					
2. Indicate case type, or identify the most important issue in the case (select only 1):					
Civil			Family Law		
Contract <i>Debt/Contract</i> <input type="checkbox"/> Consumer/DTPA <input type="checkbox"/> Debt/Contract <input type="checkbox"/> Fraud/Misrepresentation <input type="checkbox"/> Other Debt/Contract: _____ <i>Foreclosure</i> <input type="checkbox"/> Home Equity—Expedited <input type="checkbox"/> Other Foreclosure <input type="checkbox"/> Franchise <input type="checkbox"/> Insurance <input type="checkbox"/> Landlord/Tenant <input type="checkbox"/> Non-Competition <input type="checkbox"/> Partnership <input type="checkbox"/> Other Contract: _____	Injury or Damage <input type="checkbox"/> Assault/Battery <input type="checkbox"/> Construction <input type="checkbox"/> Defamation <i>Malpractice</i> <input type="checkbox"/> Accounting <input type="checkbox"/> Legal <input type="checkbox"/> Medical <input type="checkbox"/> Other Professional Liability: _____ <input type="checkbox"/> Motor Vehicle Accident <input type="checkbox"/> Premises <i>Product Liability</i> <input type="checkbox"/> Asbestos/Silica <input type="checkbox"/> Other Product Liability List Product: _____ <input checked="" type="checkbox"/> Other Injury or Damage: _____	Real Property <input type="checkbox"/> Eminent Domain/Condemnation <input type="checkbox"/> Partition <input type="checkbox"/> Quiet Title <input type="checkbox"/> Trespass to Try Title <input type="checkbox"/> Other Property: _____ Related to Criminal Matters <input type="checkbox"/> Expunction <input type="checkbox"/> Judgment Nisi <input type="checkbox"/> Non-Disclosure <input type="checkbox"/> Seizure/Forfeiture <input type="checkbox"/> Writ of Habeas Corpus—Pre-indictment <input type="checkbox"/> Other: _____	Marriage Relationship <input type="checkbox"/> Annulment <input type="checkbox"/> Declare Marriage Void <i>Divorce</i> <input type="checkbox"/> With Children <input type="checkbox"/> No Children Other Family Law <input type="checkbox"/> Enforce Foreign Judgment <input type="checkbox"/> Habeas Corpus <input type="checkbox"/> Name Change <input type="checkbox"/> Protective Order <input type="checkbox"/> Removal of Disabilities of Minority <input type="checkbox"/> Other: _____	Post-judgment Actions (non-Title IV-D) <input type="checkbox"/> Enforcement <input type="checkbox"/> Modification—Custody <input type="checkbox"/> Modification—Other Title IV-D <input type="checkbox"/> Enforcement/Modification <input type="checkbox"/> Paternity <input type="checkbox"/> Reciprocity (UIFSA) <input type="checkbox"/> Support Order Parent-Child Relationship <input type="checkbox"/> Adoption/Adoption with Termination <input type="checkbox"/> Child Protection <input type="checkbox"/> Child Support <input type="checkbox"/> Custody or Visitation <input type="checkbox"/> Gestational Parenting <input type="checkbox"/> Grandparent Access <input type="checkbox"/> Parentage/Paternity <input type="checkbox"/> Termination of Parental Rights <input type="checkbox"/> Other Parent-Child: _____	
Employment <input type="checkbox"/> Discrimination <input type="checkbox"/> Retaliation <input type="checkbox"/> Termination <input type="checkbox"/> Workers' Compensation <input type="checkbox"/> Other Employment: _____	Other Civil <input type="checkbox"/> Administrative Appeal <input type="checkbox"/> Antitrust/Unfair Competition <input type="checkbox"/> Code Violations <input type="checkbox"/> Foreign Judgment <input type="checkbox"/> Intellectual Property <input type="checkbox"/> Lawyer Discipline <input type="checkbox"/> Perpetuate Testimony <input type="checkbox"/> Securities/Stock <input type="checkbox"/> Tortious Interference <input type="checkbox"/> Other: _____				
Tax <input type="checkbox"/> Tax Appraisal <input type="checkbox"/> Tax Delinquency <input type="checkbox"/> Other Tax	Probate & Mental Health <i>Probate/Wills/Intestate Administration</i> <input type="checkbox"/> Dependent Administration <input type="checkbox"/> Independent Administration <input type="checkbox"/> Other Estate Proceedings <input type="checkbox"/> Guardianship—Adult <input type="checkbox"/> Guardianship—Minor <input type="checkbox"/> Mental Health <input type="checkbox"/> Other: _____				
3. Indicate procedure or remedy, if applicable (may select more than 1):					
<input type="checkbox"/> Appeal from Municipal or Justice Court <input type="checkbox"/> Arbitration-related <input type="checkbox"/> Attachment <input type="checkbox"/> Bill of Review <input type="checkbox"/> Certiorari <input type="checkbox"/> Class Action		<input type="checkbox"/> Declaratory Judgment <input type="checkbox"/> Garnishment <input type="checkbox"/> Interpleader <input type="checkbox"/> License <input type="checkbox"/> Mandamus <input type="checkbox"/> Post-judgment		<input type="checkbox"/> Prejudgment Remedy <input type="checkbox"/> Protective Order <input type="checkbox"/> Receiver <input type="checkbox"/> Sequestration <input type="checkbox"/> Temporary Restraining Order/Injunction <input type="checkbox"/> Turnover	



I, Marilyn Burgess, District Clerk of Harris County, Texas certify that this is a true and correct copy of the original record filed and or recorded in my office, electronically or hard copy, as it appears on this date.

Witness my official hand and seal of office this September 30, 2024

Certified Document Number: 116235799 Total Pages: 1

Marilyn Burgess, DISTRICT CLERK
HARRIS COUNTY, TEXAS

In accordance with Texas Government Code 51.301 and 406.013 electronically transmitted authenticated documents are valid. If there is a question regarding the validity of this document and or seal please e-mail support@hcdistrictclerk.com